Cisco Support Community

Expert Series Webcast

DMVPN Fase1 y 2 en IPv4: Fundamentos y Configuración básica enfocado al CCIE R&S

Gustavo Salazar

Ingeniero consultor de Tecnologías de la Información y Desarrollador de Políticas de Enrutamiento y Seguridad

Instructor de Cisco Network Academy

Diciembre 2016

@Gusdsalazar

La tecnología nunca deja de avanzar
¡Conoce la opinión de los expertos!

Comunidad de Soporte de Cisco en Español
http://cs.co/90098DJFB

©2016 Cisco and/or its affiliates. All rights reserved.

Califique el contenido de la Comunidad de Soporte en Español.

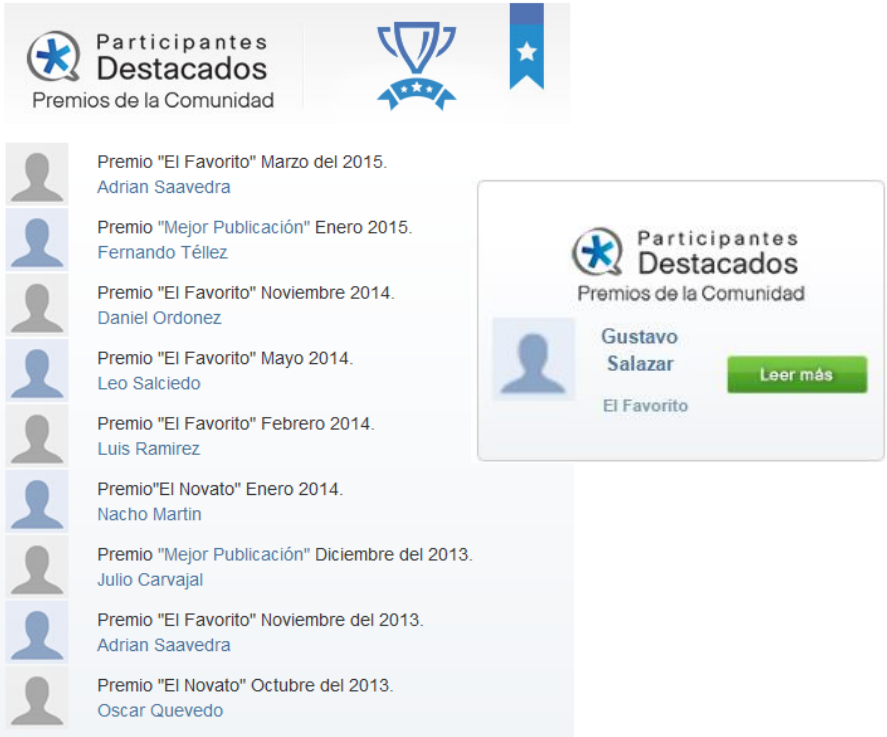
Ahora puede calificar discusiones, documentos, blogs y videos!!...

Esto es con el fin de que nos ayude a distinguir contenido de calidad y también para reconocer los esfuerzos de los integrantes de la Comunidad de Soporte de Cisco en español.

©2016 Cisco and/or its affiliates. All rights reserved.

Reconocimientos en la comunidad

El reconocimiento al **“Participante Destacado de la Comunidad”** está diseñado para reconocer y agradecer a aquellas personas que colaboran con contenido técnico de calidad y ayudan a posicionar nuestra comunidad como el sitio número uno para las personas interesadas en tecnología Cisco.



©2016 Cisco and/or its affiliates. All rights reserved.

Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.
Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión

©2016 Cisco and/or its affiliates. All rights reserved.

Expert Series Webcast

DMVPN Fase1 y 2 en IPv4: Fundamentos y Configuración básica enfocado al CCIE R&S

Gustavo Salzar es consultor de Tecnologías de la Información y Desarrollador de Políticas de Enrutamiento y Seguridad en tecnologías Cisco. Es instructor de Cisco Network Academy, es el mejor instructor del año en Latino América y un Cisco Champion de 2016. Es docente universitario a nivel maestría de la Universidad de las Fuerzas Armadas-ESPE. Gustavo es originario de Ecuador y cuenta con diversas certificaciones como: CCNA Security, Cisco IOS Security Specialist, CCDA, CCDP, CCNP R&S e IPv6 Forum Gold Engineer entre otras.

Gustavo Salazar

©2016 Cisco and/or its affiliates. All rights reserved.

Question Manager

Enrique Ramírez

Enterprise Architect

©2016 Cisco and/or its affiliates. All rights reserved.

Gracias por estar con nosotros hoy dia!

Si desea obtener la presentación de este evento diríjase a:

http://cs.co/90058zdbt

©2016 Cisco and/or its affiliates. All rights reserved.

¡Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.

©2016 Cisco and/or its affiliates. All rights reserved.

DMVPN Fase 1 y Fase 2 en IPv4

Fundamentos y Configuración Básica enfocado al CCIE R&S

Tomorrow Starts Here

Ing. Gustavo Salazar, MSc.

Mejor Graduado de todos los posgrados PUCE 2014-2015
ITQ Instructor – CCNA R&S, CCNA Security, CCNP R&S, IT Essentials
Mejor Instructor Cisco Networking Academy Latinoamérica 2016
CCDA, CCDP, Cisco IOS Security Specialist
CCIE R&S Candidate – Cisco Champion 2016

Agenda

1. Fundamentos de DMVPN: Definición y Beneficios
2. Componentes principales
3. Comandos necesarios para su configuración
4. Consideraciones Importantes para el Enrutamiento con EIGRP y OSPF
5. Implementación y Verificación – Demo en Vivo: DMVPN Fase 2 /w IPsec
6. Q&A

Pregunta 1

¿Cuál es su nivel actual de conocimientos en Routing and Switching?

A. No tengo ningún conocimiento de redes
B. Inicial (Nivel CCENT)
C. Asociado (Nivel CCNA R&S)
D. Profesional (Nivel CCNP R&S)
E. Experto (Nivel CCIE R&S)

CCIE R&S Blueprint (Written and Lab)

CCIE R&S Written Exam (400-101) v5.1

- ✓ Duración: 120 min. (más 30 min de tiempo extendido)
- ✓ Cantidad de Preguntas: 90 a 110
- ✓ Tópicos: https://learningnetwork.cisco.com/community/certifications/ccie_routing_switching/written_exam_v5/exam-topics

1.0 Network Principles	10%
2.0 Layer 2 Technologies	13%
3.0 Layer 3 Technologies	37%
4.0 VPN Technologies	13%
5.0 Infrastructure Security	5%
6.0 Infrastructure Services	12%
7.0 Evolving Technologies	10%

CCIE R&S Blueprint (Written and Lab)

CCIE R&S Written Exam (400-101) v5.1

- ✓ Duración: 120 min. (más 30 min de tiempo extendido)
- ✓ Cantidad de Preguntas: 90 a 110
- ✓ Tópicos: https://learningnetwork.cisco.com/community/certifications/ccie_routing_switching/written_exam_v5/exam-topics

- 4.1.d Implement and troubleshoot DMVPN [single hub]
  - 4.1.d [i] NHRP
  - 4.1.d [ii] DMVPN with IPsec using preshared key

CCIE R&S Blueprint (Written and Lab)

CCIE R&S Lab

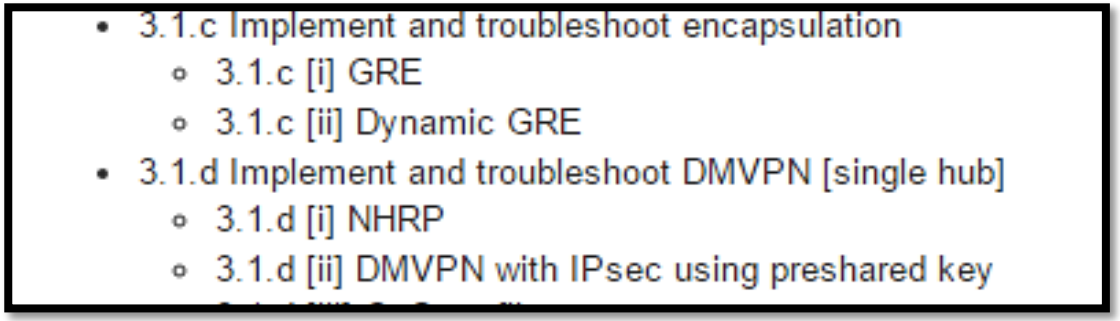
- ✓ Estructura del Examen:
  El examen CCIE R&S Lab consiste en una sección de Troubleshooting de 2 horas, Una sección de Diagnóstico de 30 minutos y finalmente 5 horas y media de Configuración.
- ✓ Tópicos:
  https://learningnetwork.cisco.com/community/certifications/ccie_routing_switching/lab_exam_v5/exam-topics

1.0 Layer 2 Technologies	20%
2.0 Layer 3 Technologies	40%
3.0 VPN Technologies	20%
4.0 Infrastructure Security	5%
5.0 Infrastructure Services	15%

CCIE R&S Blueprint (Written and Lab)

CCIE R&S Lab

- ✓ Estructura del Examen:
  El examen CCIE R&S Lab consiste en una sección de Troubleshooting de 2 horas, Una sección de Diagnóstico de 30 minutos y finalmente 5 horas y media de Configuración.
- ✓ Tópicos:
  https://learningnetwork.cisco.com/community/certifications/ccie_routing_switching/lab_exam_v5/exam-topics



- 3.1.c Implement and troubleshoot encapsulation
  - 3.1.c [i] GRE
  - 3.1.c [ii] Dynamic GRE
- 3.1.d Implement and troubleshoot DMVPN [single hub]
  - 3.1.d [i] NHRP
  - 3.1.d [ii] DMVPN with IPsec using preshared key

CCIE R&S Blueprint (Written and Lab)

CCNA R&S 200-125 – ICND 2 200-105

- ✓ La certificación actual CCNA R&S cubre ya el tema de DMVPN de forma teórica, además de incluir a GRE VPN (y una breve introducción a IPsec).

Fundamentos de DMVPN: Definición y Beneficios

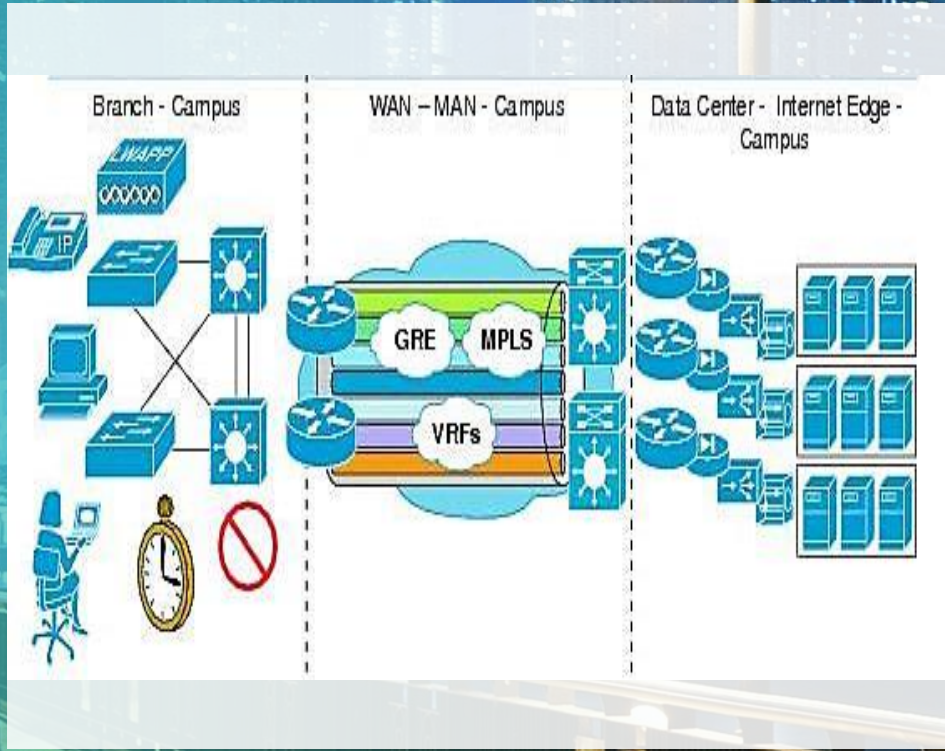
Cisco Confidential

Necesidades de las Empresas Modernas

Implementaciones de conectividad para medianas o grandes empresas (Matriz – Sucursales) requieren el soporte de servicios IP avanzados para satisfacer sus necesidades:

- **IP Multicast:** *Requerido para el envío eficiente y escalable en comunicaciones one-to-many (Internet Broadcast)* y many-to-many (Videoconferencias) especialmente con tráfico de Video, voz y aplicaciones críticas empresariales (QoS)
- **Uso de Protocolos de Enrutamiento Dinámico** para disminuir la carga administrativa en entornos donde el enrutamiento estático no es manejable u óptimo
- Tradicionalmente esto se lograba con Túneles estáticos (como GRE) y encriptándolos con IPsec, pero con problemas en su implementación y complejidad en entornos Multicast = Ineficiencia.

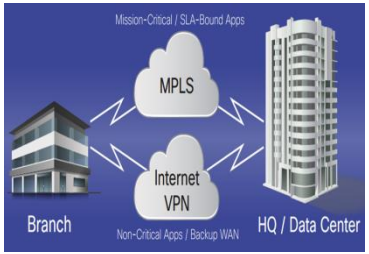
Cisco DMVPN combina el tunelamiento GRE con la encriptación IPsec y *Next-Hop Resolution Protocol* (NHRP) en una manera que cumple esos requerimientos, reduciendo la carga administrativa



Fundamentos de DMVPN: Caraterísticas

Características	Implicación
Cisco Dynamic Multipoint VPN es una solución implementada en equipos Cisco con IOS (Cisco IOS Software-Base Solution) ampliamente usada para conectividad empresarial escalable	Solución implementada en equipos Cisco con IOS como O.S. (No es posible implementarlo en ASAs por ejemplo) para unir la Matriz con sucursales, teletrabajadores y extranets.
Ofrece conectividad segura bajo demanda con una configuración *hub-and-spoke* simple.	Generación de túneles IPsec automáticos con configuración “Zero-touch” en el Hub al añadir nuevos sitios remotos
Reducción de latencia y consumo de Ancho de Banda para aplicaciones distribuidas como voz y video	Cisco DMVPN puede implementarse en entornos de gran escala en conjunto con Cisco IOS Firewall, Cisco IOS IPS, QoS, IP Multicast.

Cisco IOS® SOFTWARE



Fundamentos de DMVPN: Reducción en la Configuración

Antes de DMVPN: p-pGRE + IPsec

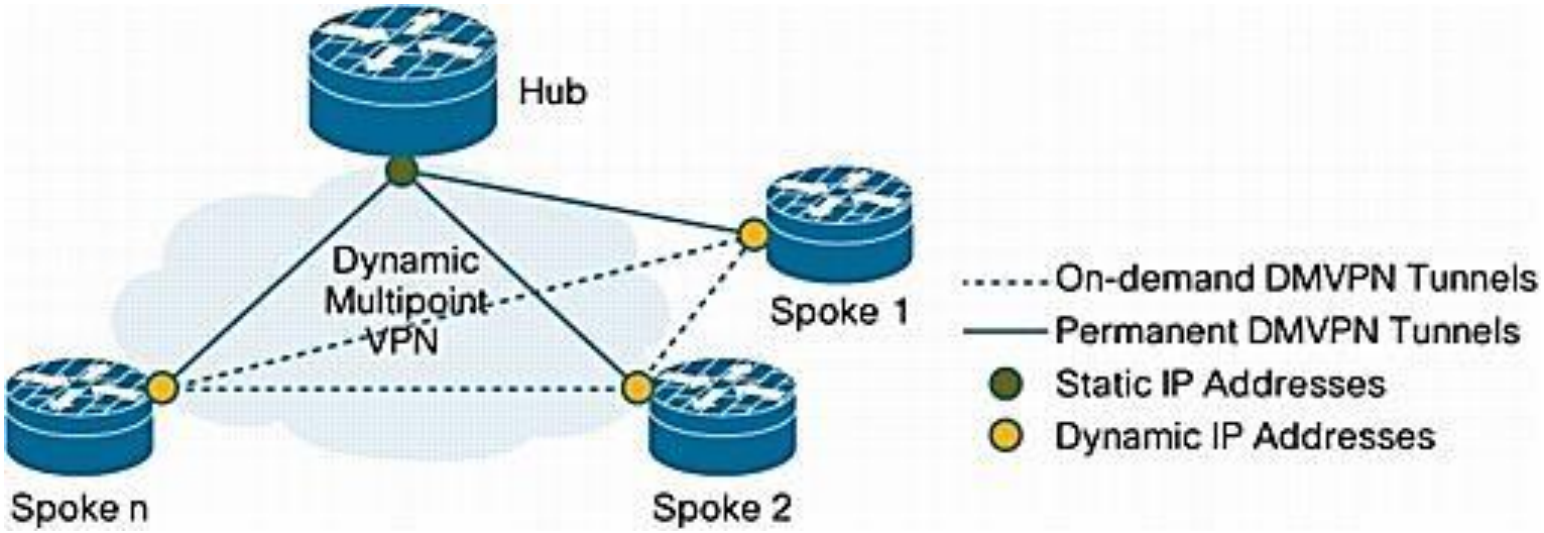
- ✓ Una interfaz túnel GRE para cada Spoke
- ✓ Todos los túneles deben ser estáticamente predefinidos
- ✓ Una gran configuración en el Hub:
  - ❑ 1 interfaz/spoke con **250 spokes** = 250 interfaces
  - ❑ 7 líneas de configuración por spoke = 1750 líneas
  - ❑ 4 Dir. IP/interfaz túnel = 1000 direcciones configuradas
- ✓ Spokes adicionales requieren configuración adicional en el Hub
- ✓ Comunicación Spoke-to-Spoke debe pasar siempre por el Hub

Fundamentos de DMVPN: Reducción en la Configuración

Con DMVPN: mGRE + IPsec

- ✓ Una sola interfaz mGRE para todos los Spokes
- ✓ Direcciones IP destino de los túneles simplifica la administración y su configuración.
- ✓ Configuración Reducida en el Hub:
  - ❑ 1 interfaz para todos los spokes (para 250 spokes) = 1 interfaz
  - ❑ Configuración con NHRP (para 250 spokes) = 15 líneas
  - ❑ 1 Dir. IP/interfaz túnel = 250 direcciones configuradas
- ✓ Spokes adicionales NO requieren más configuración en el Hub
- ✓ Comunicación Spoke-to-Spoke **puede pasar por el Hub o hacerlo directo**.

Fundamentos de DMVPN: Topología Base



Fundamentos de DMVPN: Aplicaciones

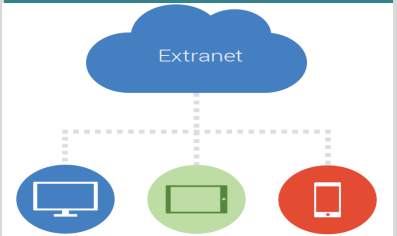
Aplicaciones de DMVPN:

Cisco DMVPN es una de las soluciones preferidas para organizaciones que requieren conectividad WAN encriptada entre una Matriz (Hub) y sitios remotos (Spokes):

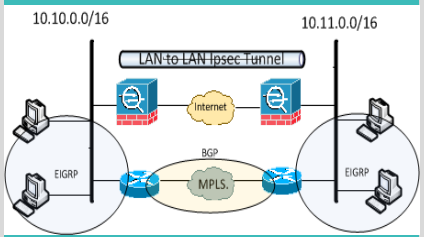
- Uso del Internet como medio WAN primario o de Backup debido a su relativo bajo costo y facilidad de acceso.
- Obligación de tener tráfico encriptado aún en enlaces dedicados WAN
- Completa integración en entornos MPLS e IPv6

Aplicaciones Críticas

Extranet Empresarial



Conexiones Backup

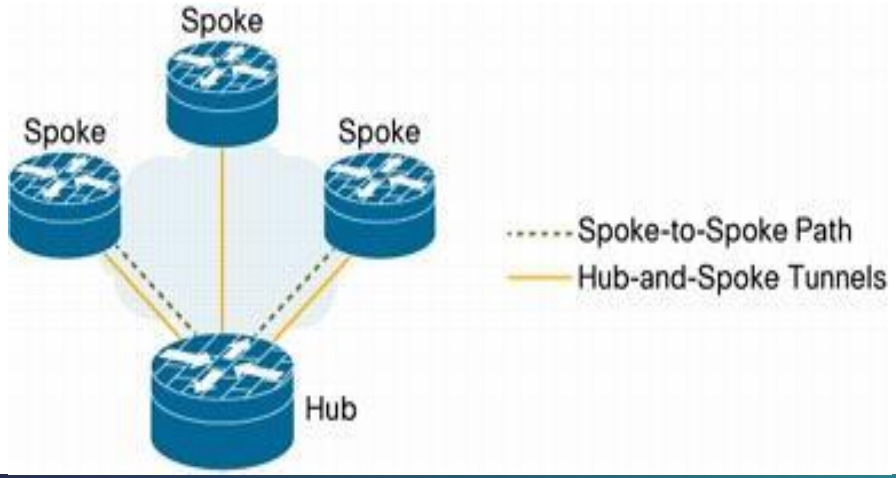


VPN para SP – Integración con VRFs

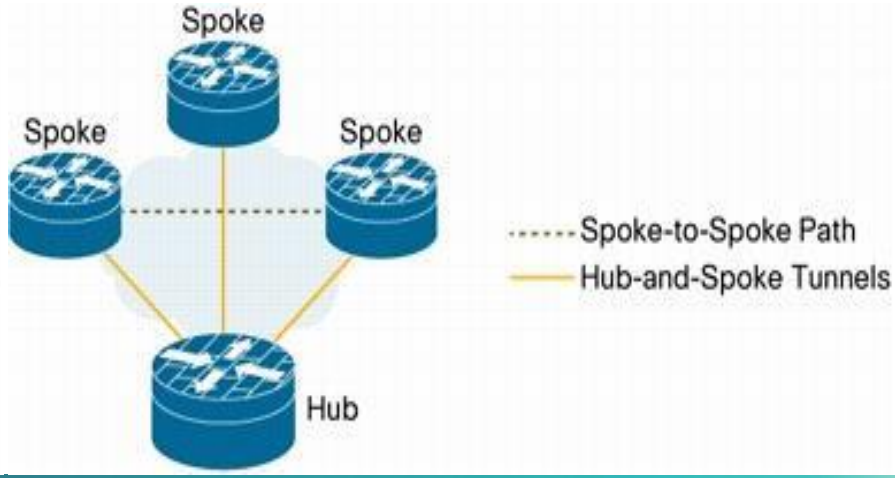
Fundamentos de DMVPN: Escenarios de Implementación

Cisco DMVPN puede implementarse en dos escenarios básicos:

1 Cisco DMVPN
Modelo Hub and Spoke



2 Cisco DMVPN
Modelo Spoke - to - Spoke



Fundamentos de DMVPN: Escenarios de Implementación

La regla 80:20 puede emplearse para determinar qué modelo usar

Modelo Hub-and-Spoke

- Si el 80% o más del tráfico desde los spokes está dirigido a la matriz (Hub), se debe emplear este modelo
- Para redes con un alto volumen de tráfico IP Multicast, este modelo es preferido

Modelo Spoke-to-Spoke

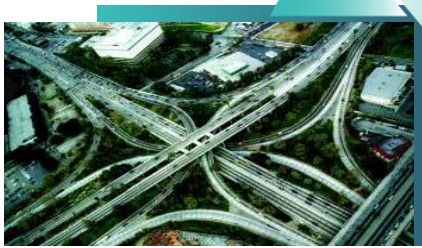
- Si más del 20% del tráfico es enviado entre sucursales (spokes), considere este modelo.

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Componentes Principales de DMVPN

Cisco Confidential

mGRE Tunnel Interface



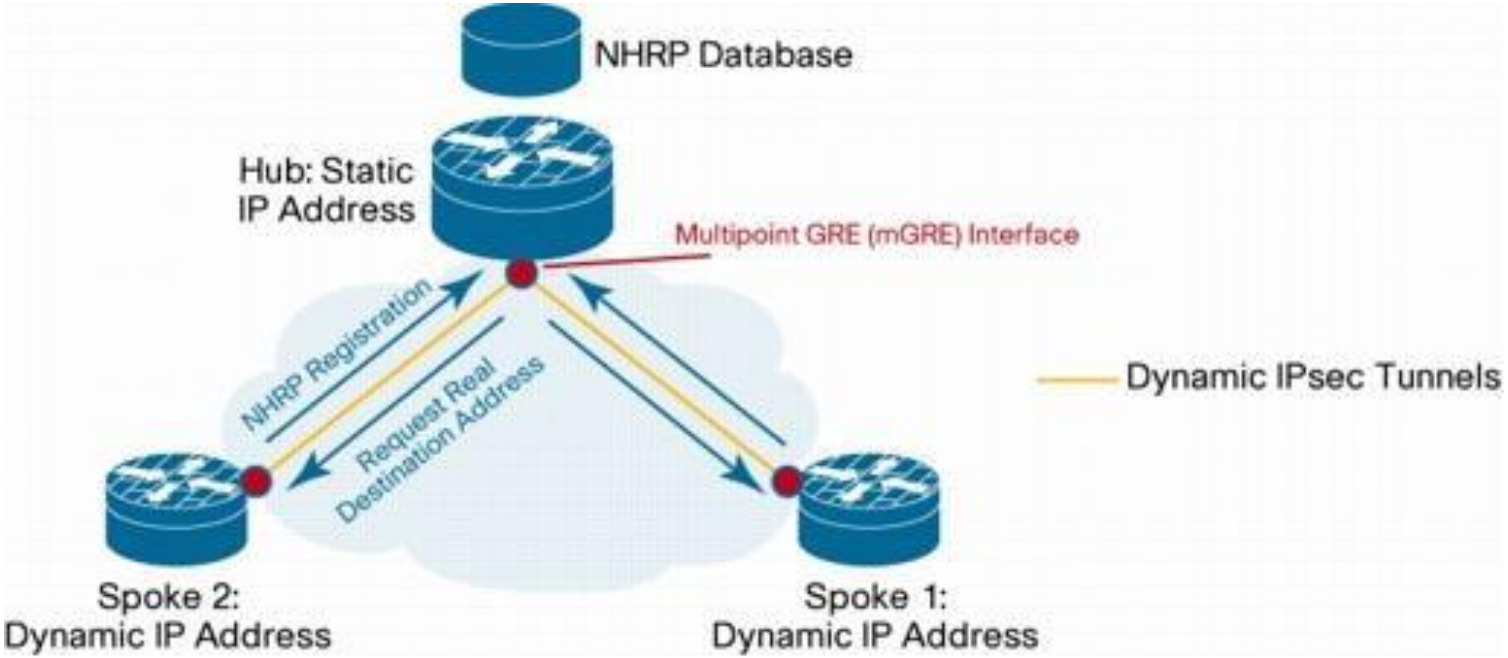
NHRP

Cisco DMVPN

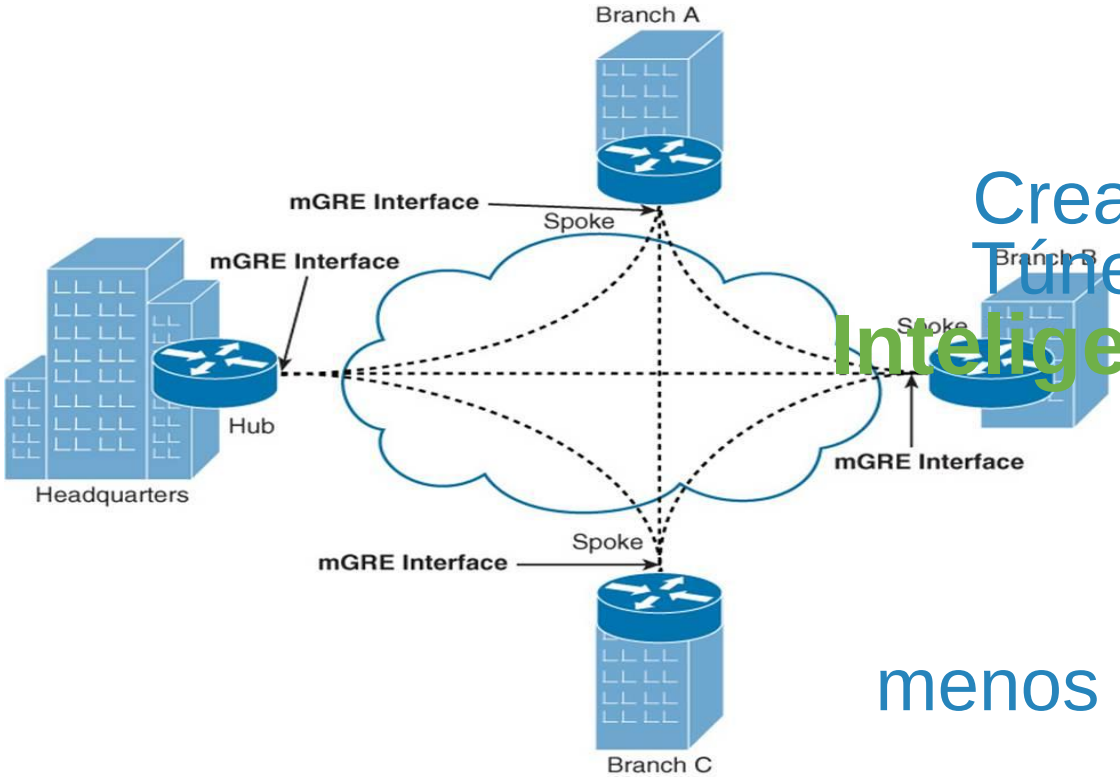
IPsec Profiles

Descubrimiento dinámico de túneles IPsec

Componentes de DMVPN: Arquitectura Básica



Componentes de DMVPN: Multipoint GRE - mGRE



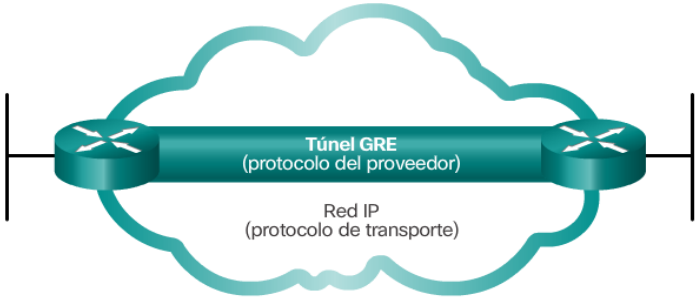
Creación Dinámica de Túneles

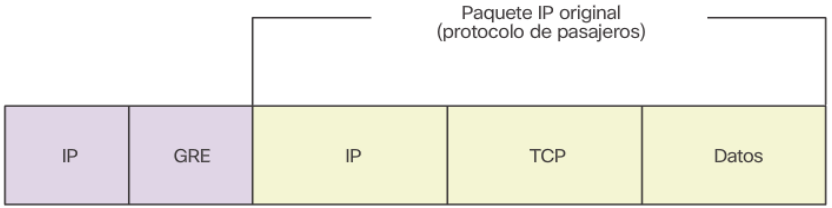
Inteligentes

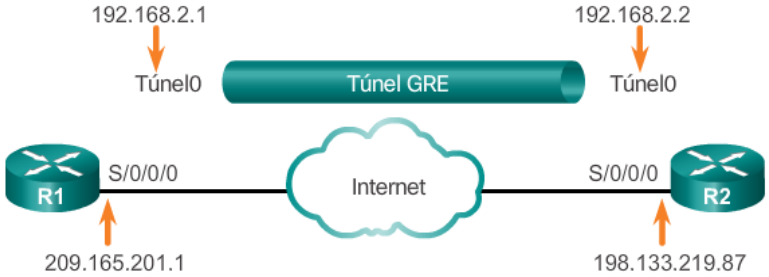
Con Seguridad Integrada y menos configuración.

Componentes de DMVPN: mGRE

GRE – Generic Routing Encapsulation







Configuración del R1:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Componentes de DMVPN: mGRE

mGRE – Multipoint Generic Routing Encapsulation

- ✓ Permite que una interfaz GRE simple soporte múltiples túneles IPsec simplificando con ello su configuración.
- ✓ Destino dinámico del túnel
  - ❑ Requiere de Next Hop Resolution Protocol (NHRP) para su formación
  - ❑ Soporte para direcciones dinámicas y NAT

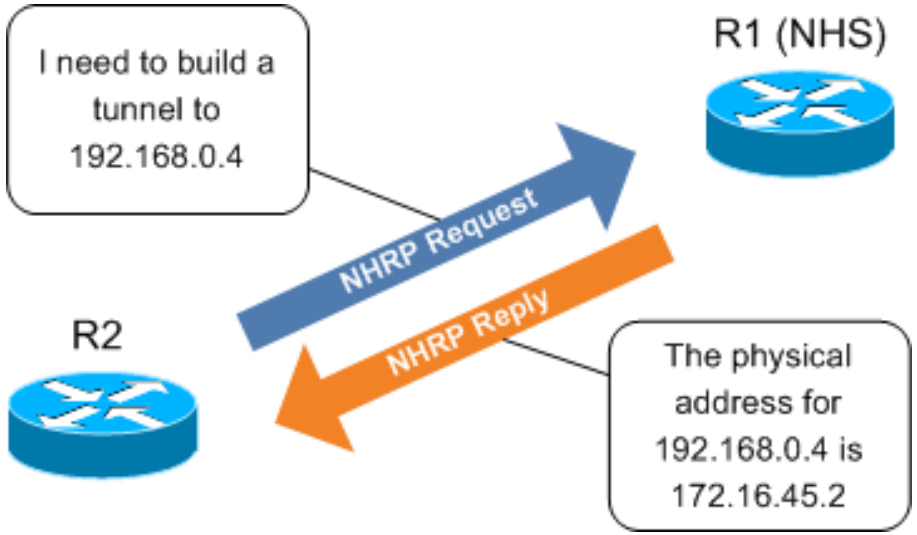
Componentes de DMVPN: NHRP (Next Hop Resolution Protocol)

NHRP – Next Hop Resolution Protocol (RFC 2332)

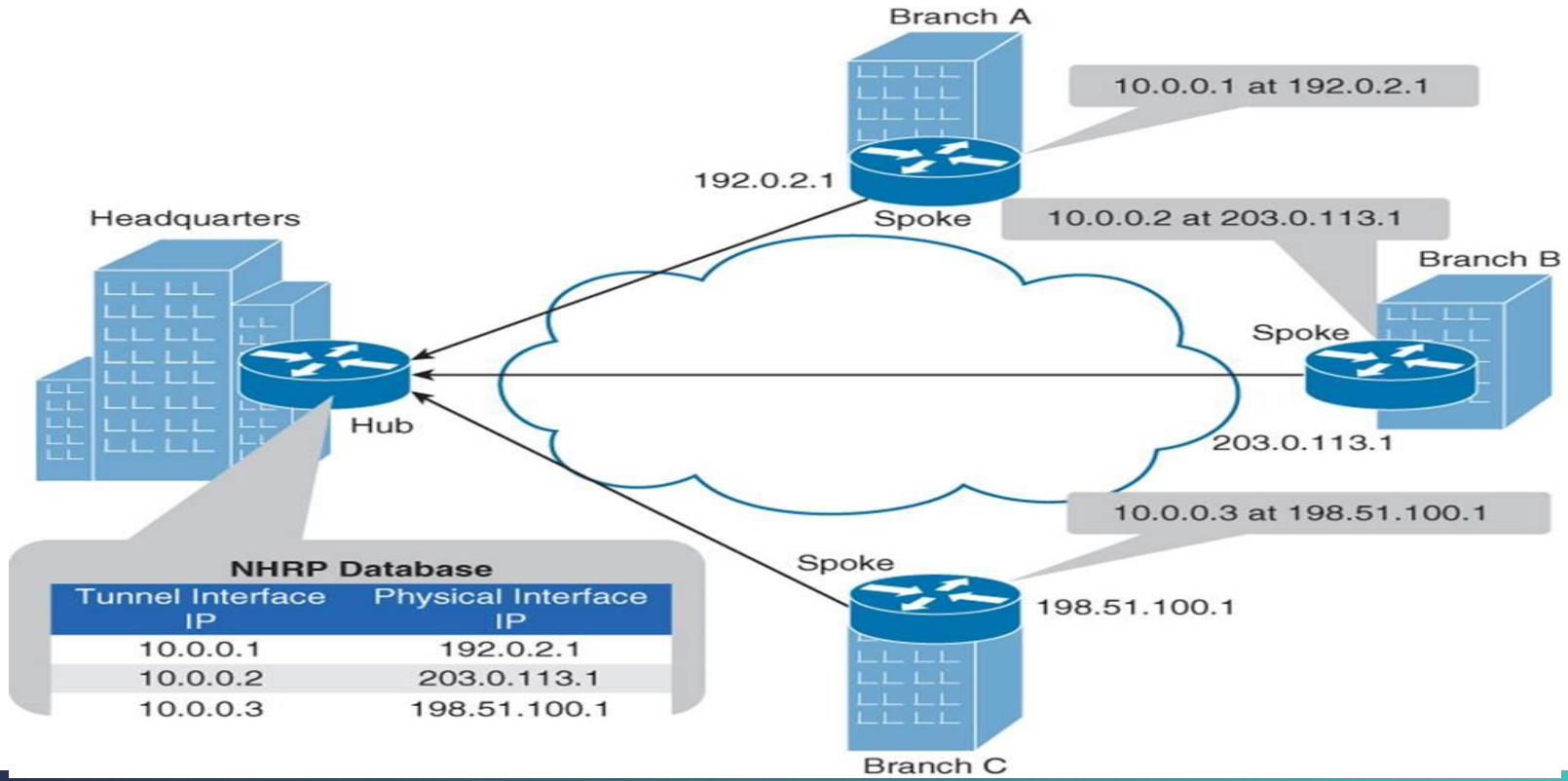
- ✓ Permite que las sucursales (spokes) estén configuradas con direcciones IP dinámicas, las cuales se obtienen mediante un proceso de solicitud/respuesta entre Hub y Spokes
- ✓ El Hub (NHS) mantiene una base de datos NHRP de dichas direcciones para cada spoke – Similar al Caché ARP:
  - ❑ Cada spoke (NHC) se registra contra el Hub cuando se enciende
  - ❑ Cuando un spoke requiere construir un túnel con otro spoke, solicita dicha dirección al Hub.

Componentes de DMVPN: NHRP (Next Hop Resolution Protocol)

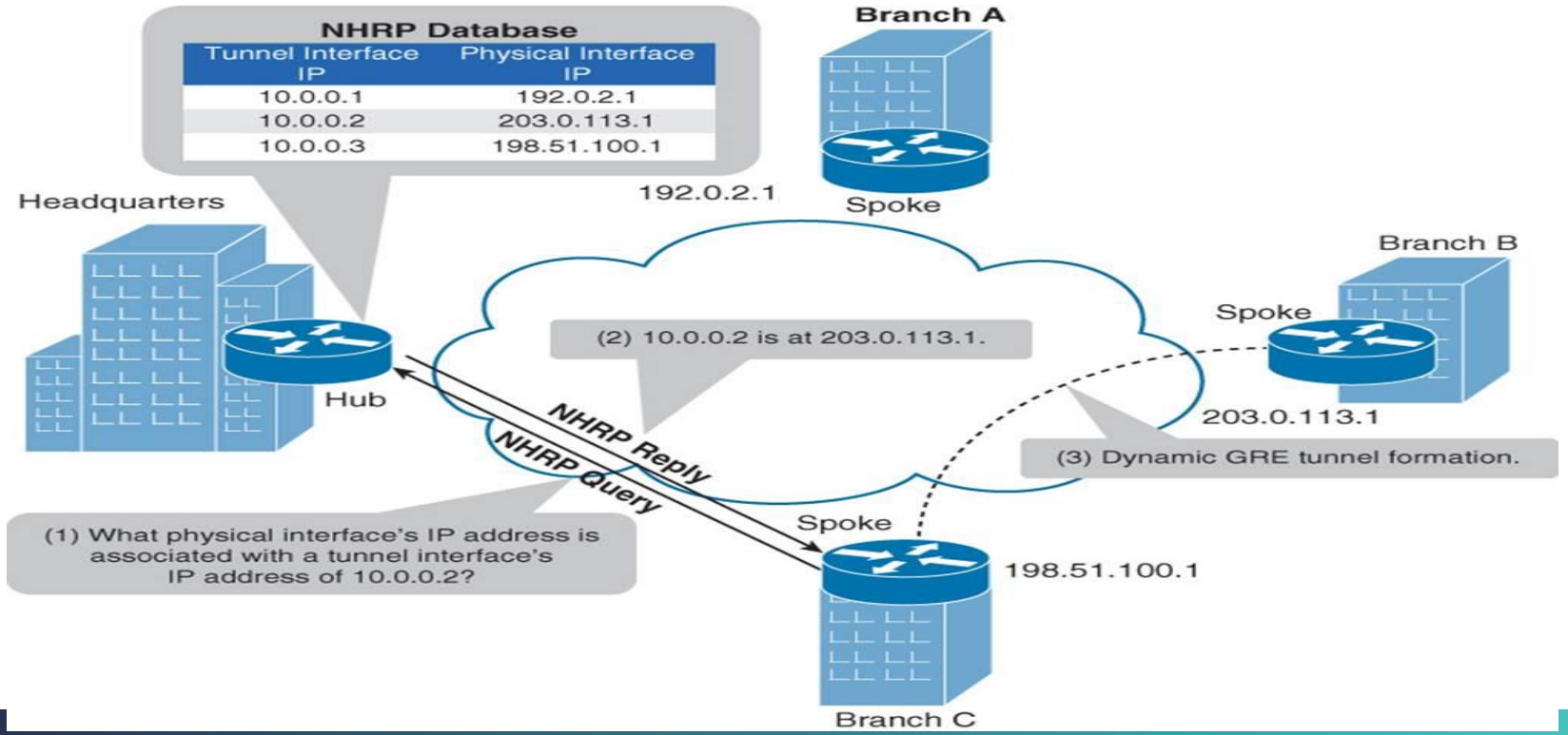
NHRP – Next Hop Resolution Protocol



Componentes de DMVPN: Proceso de registro NHRP



Componentes de DMVPN: Proceso de registro NHRP



Componentes de DMVPN: IPsec – Ataques a la Seguridad

Vulnerabilidad

- Datos basados en IP son vulnerables a ataques como *spoofing, sniffing y session highjacking* debido a la propia naturaleza de encapsulación y enrutamiento de los paquetes.

Ataques comunes

- **Spoofing** es un ataque donde un dispositivo simula ser otro en una red.
- **Sniffing** es una ataque que involucra escuchar sin autorización una transmisión de datos (eavesdropping)
- **Session Hijacking** es un ataque en el que un cracker usa tanto **spoofing** como **sniffing** para ingresar a una sesión previamente iniciada

IPsec - IETF

- En cada una de esas formas de ataques de red, un ente no autorizado gana acceso a la información privada de una compañía.
- Para remediar ese problema, la IETF creó la **suite de protocolos IPsec**, conjunto de protocolos que proveen servicios de seguridad a nivel de capa de red. IPsec está basado en tecnologías criptográficas que aseguran su autenticación y privacidad (originalmente definido en los RFCs 1825 a 1829)

Componentes de DMVPN: IPsec

La idea de concebir una red segura, debe empezar con una **adecuada política de seguridad** y así dictaminar cómo implementar dicha seguridad en la red.

Cisco Systems ofrece muchas soluciones tecnológicas en el ámbito de seguridad tanto para el acceso a Internet, Extranet y accesos remotos.

Una de dichas soluciones es emplear IPsec, siendo éste un elemento clave para una solución de seguridad total, ofreciendo **Privacidad, Integridad y autenticación** para transmitir datos sensibles sobre redes inseguras o públicas de forma transparente en la infraestructura sin afectar a host individuales.

Componentes de DMVPN: IPsec

Funciones de IPsec

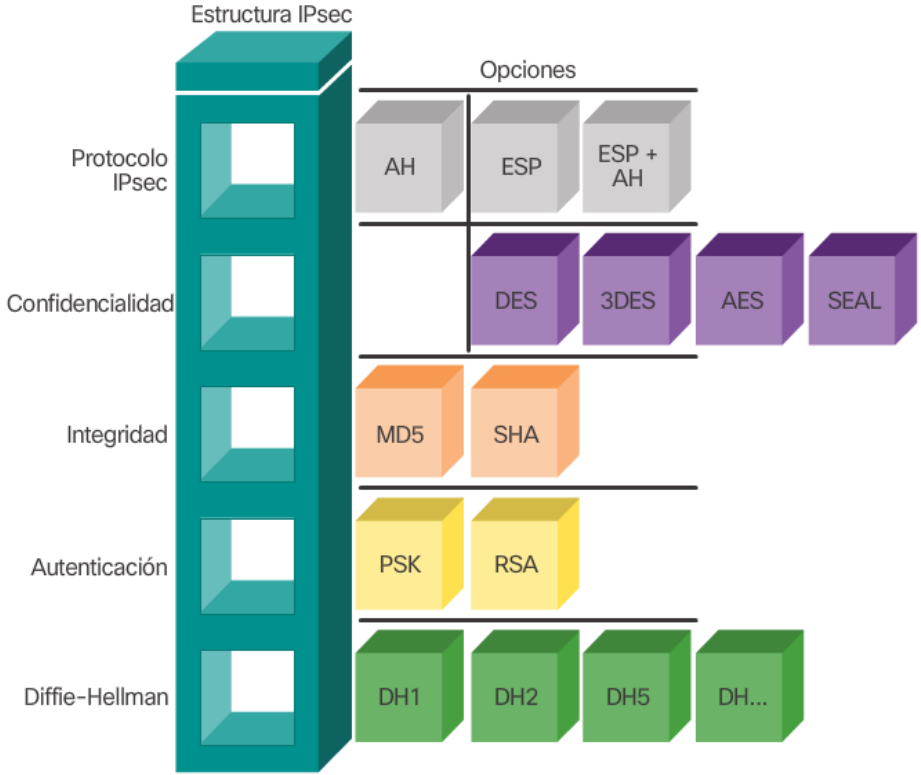
Confidencialidad

Integridad de datos

Autenticación

16	24	32 bit
Identificador de asociación de seguridad (SPI)		
Número de secuencia		
Datos del contenido (longitud variable)		
Relleno (de 0bytes a 255bytes)		
	Longitud del relleno	Siguiente encabezado
Datos de autenticación (variable)		

Protección antirreproducción

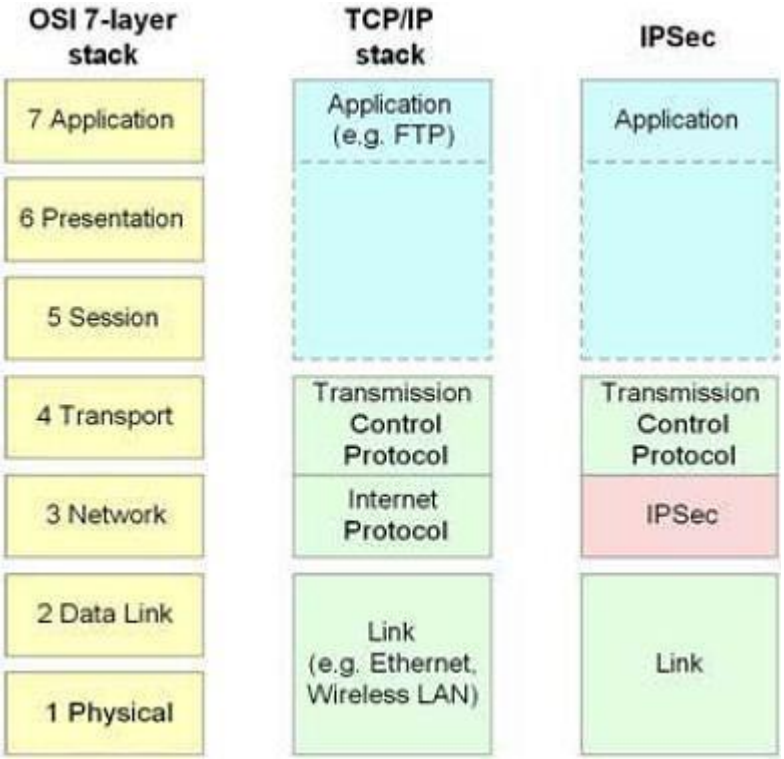


Componentes de DMVPN: Beneficios de IPsec

Los beneficios principales de IPsec son:

- Cuando IPsec es implementado en un firewall o en un router, esta tecnología provee una seguridad fuerte que puede ser aplicada a todo el tráfico que cruzará el perímetro. Cabe aclarar que el tráfico interno al perímetro no se verá afectado por el procesamiento y overhead relacionado con IPsec.
- IPsec se ubica bajo la capa de transporte del modelo OSI (TCP/UDP), por lo que es transparente a las aplicaciones y a los usuarios finales

Componentes de DMVPN: Beneficios de IPsec



Componentes de DMVPN: Alcance de IPsec

IPsec provee tres formas de aplicarlo:

Solo autenticación

- Uso del encabezado AH (Authentication Header)

Combinación de autenticación y encriptación

- Función denominada ESP (Encapsulating Security Payload)

Función de Intercambio de llaves

- Para VPNs, tanto la autenticación como la encriptación de datos son deseados, pero se debe incluir un buen manejo de intercambio de llaves

AH o ESP?

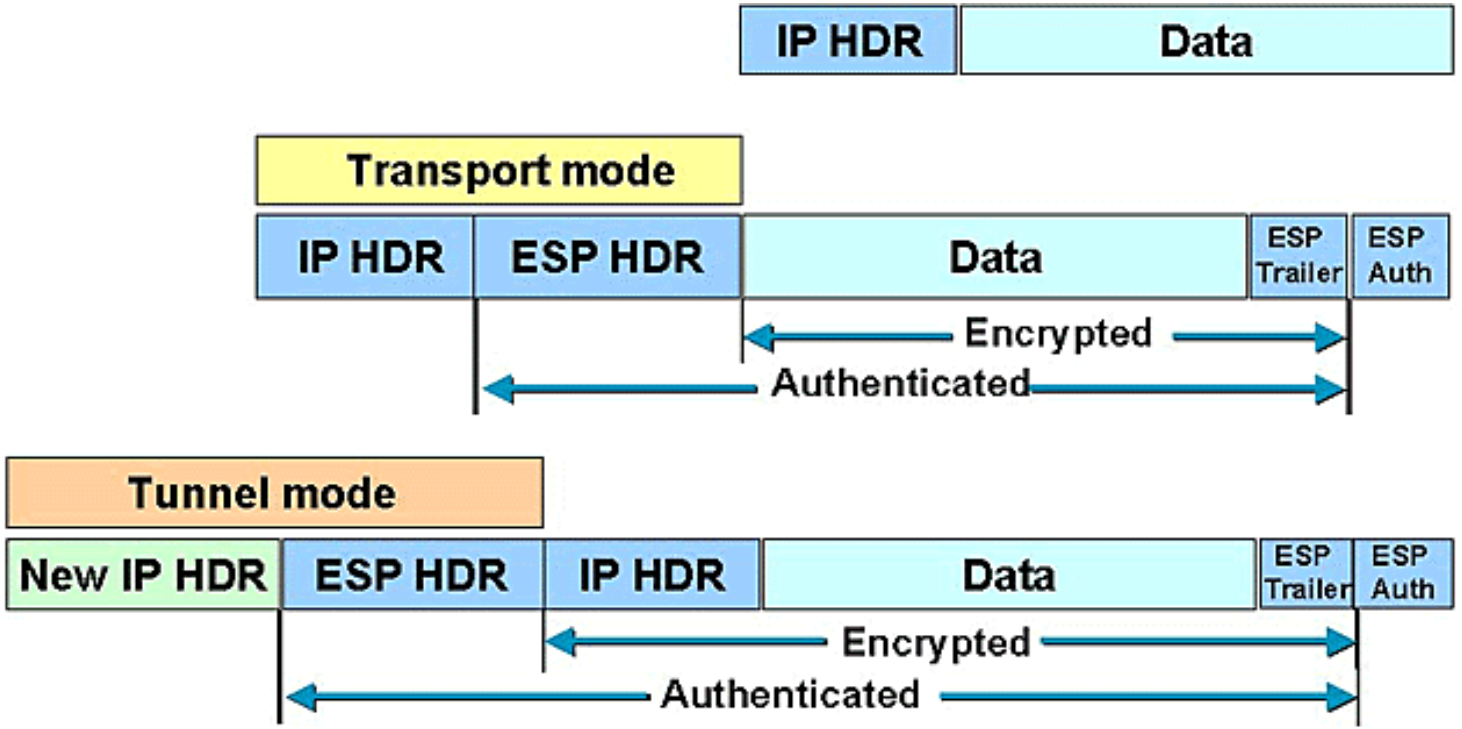
- Debido a que tanto la autenticación como la encriptación son necesarias en las transmisiones de datos modernas, es más usado ESP que AH.
- La función de intercambio de llaves puede ser manual o automatizado

Componentes de DMVPN: Modos de Encriptación de IPsec

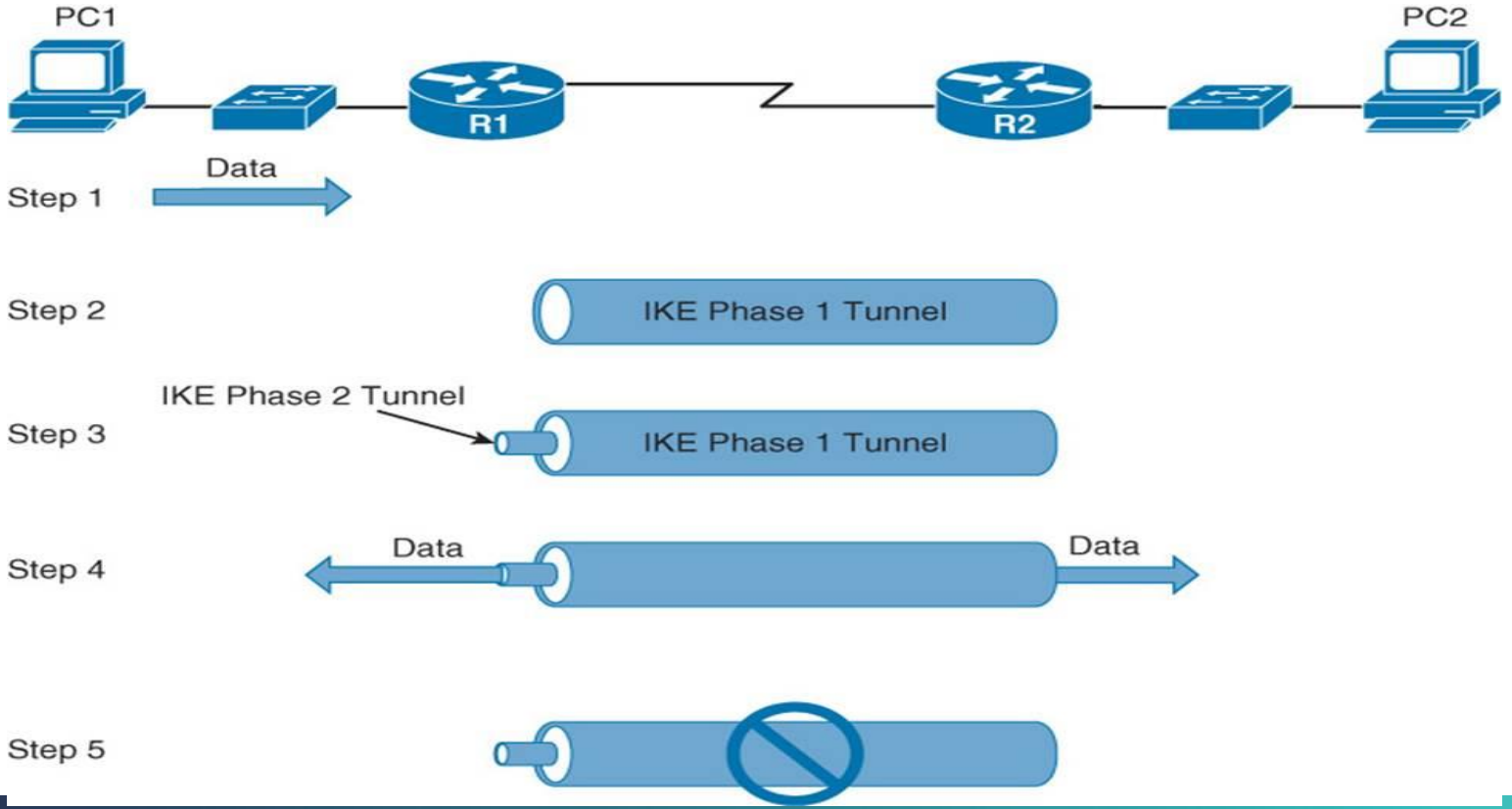
IPsec soporta dos modos de encriptación:

- **Modo de Transporte:** Encripta solo el payload (datos) de cada paquete y se deja el encabezado original. Este modo es aplicable tanto en implementaciones site-to-site como implementaciones directamente desde el cliente.
- **Modo Túnel:** Es más seguro que el modo de transporte ya que encripta tanto el payload como los encabezados. IPsec modo túnel es usado normalmente cuando la seguridad es provista por un dispositivo que no origina la información (Site-to-Site VPN).

Componentes de DMVPN: Modos de Encriptación de IPsec



Componentes de DMVPN: Tecnología IPsec



Pregunta 2

¿Tiene conocimientos de conectividad usando VPNs?

A. Si
B. No
C. Muy Poco

Comandos necesarios para la configuración de DMVPN (CCIE R&S)

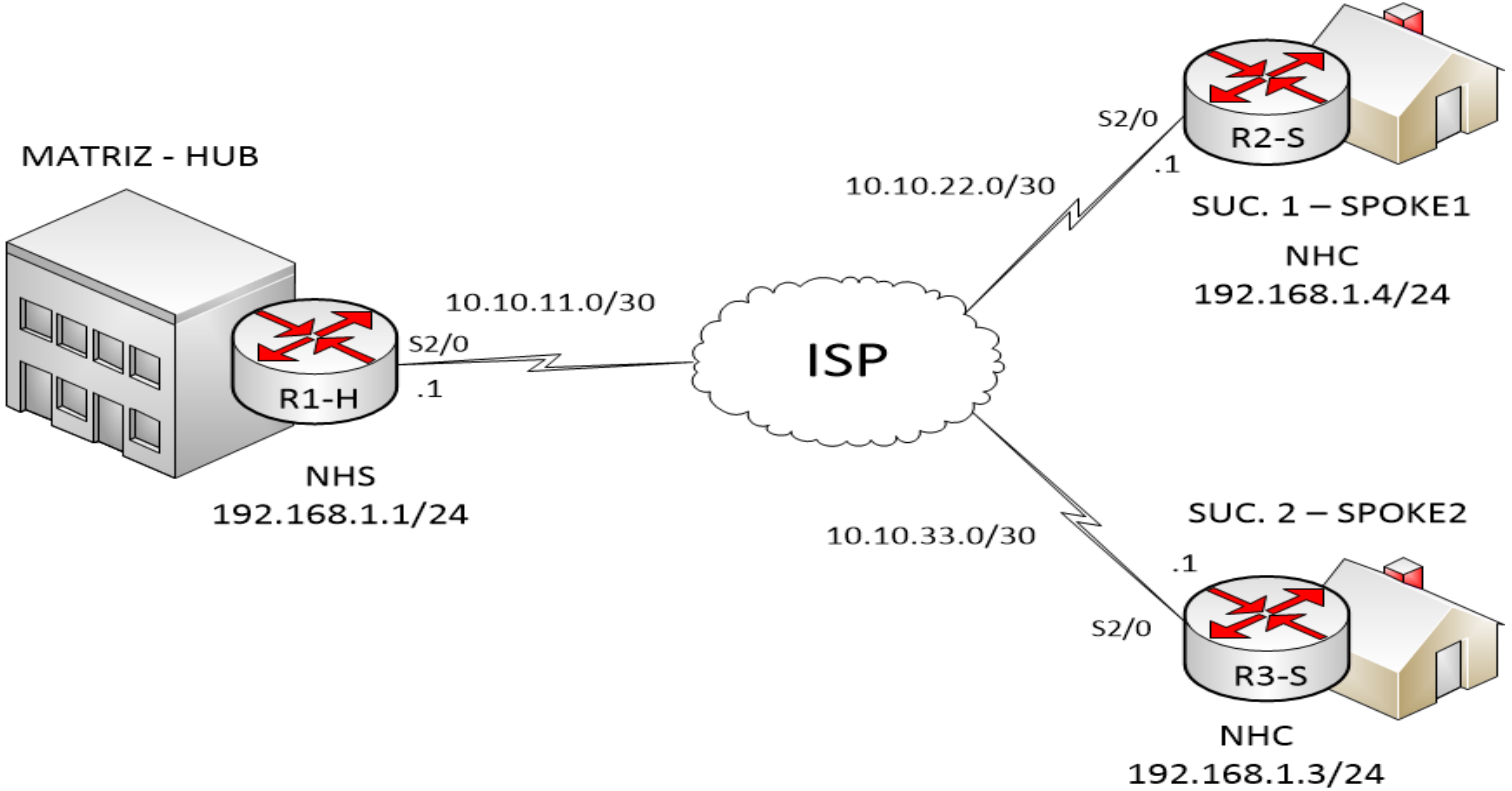
Cisco Confidential

Configuración de DMVPN: Fases DMVPN

DMVPN puede ser configurado en tres diferentes fases:

- ✓ **Fase 1:** Conectividad sólo Hub-Spoke
- ✓ **Fase 2:** Se añade capacidad de conexión Spoke a Spoke
- ✓ **Fase 3:** Se brinda mejoras a la comunicación Spoke a Spoke

Configuración de DMVPN: Topología de Referencia



Configuración de DMVPN: Fase 1 DMVPN

Configuración **HUB:**

```
R1-H(config)#int tunnel 1
R1-H(config-if)#ip add 192.168.1.1 255.255.255.0
R1-H(config-if)#tunnel source s2/0
R1-H(config-if)#tunnel mode gre multipoint
R1-H(config-if)#ip nhrp network-id 123
```

Configuración **SPOKE**

```
R2-S(config)#int tunnel 1
R2-S(config-if)#ip add 192.168.1.2 255.255.255.0
R2-S(config-if)#tunnel source s2/0
R2-S(config-if)#tunnel destination 10.10.11.1
R2-S(config-if)#ip nhrp network-id 213
R2-S(config-if)#ip nhrp nhs 192.168.1.1
R2-S(config-if)#ip nhrp map 192.168.1.1 10.10.11.1
```

Configuración de DMVPN: Fase 2 DMVPN

- ✓ En esta fase, los **spokes** remueven las direcciones de destino del túnel y se convierten en interfaz mGRE
- ✓ Los **spokes** determinan la dirección física de destino del túnel mediante NHRP
- ✓ La configuración en el **Hub** es la misma que en la fase 1

Configuración **Spoke:**

```
R2-S(config)#int tunnel 1
R2-S(config-if)#ip add 192.168.1.2 255.255.255.0
R2-S(config-if)#tunnel source s2/0
R2-S(config-if)#tunnel mode gre multipoint
R2-S(config-if)#ip nhrp network-id 213
R2-S(config-if)#ip nhrp nhs 192.168.1.1
R2-S(config-if)#ip nhrp map 192.168.1.1 10.10.11.1
```

Configuración de DMVPN: Fase 2 DMVPN

- ✓ Verificación de creación dinámica de túneles hacia los spokes

```
R1-H#show dmvpn
  # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
  ----- --------------- --------------- ----- -------- -----
      1 10.10.22.2          192.168.1.2    UP 02:47:23     D
      1 10.10.33.3          192.168.1.2    UP 03:00:19     D
```

Configuración de DMVPN: Fase 3 DMVPN

- ✓ En esta fase, se mejora la comunicación entre spokes (redirect y shortcut)
  - ❑ **Redirect** da al spoke el camino óptimo para alcanzar los otros spokes de forma directa
  - ❑ **Shortcut** permite al spoke procesar información de redirección desde el hub

Configuración de DMVPN: Fase 3 DMVPN

Configuración **HUB:**

```
R1-H(config)#int tunnel 1
R1-H(config-if)#ip add 192.168.1.1 255.255.255.0
R1-H(config-if)#tunnel source s2/0
R1-H(config-if)#tunnel mode gre multipoint
R1-H(config-if)#ip nhrp network-id 123
R1-H(config-if)#ip nhrp redirect
```

Configuración **SPOKE**

```
R2-S(config)#int tunnel 1
R2-S(config-if)#ip add 192.168.1.2 255.255.255.0
R2-S(config-if)#tunnel source s2/0
R2-S(config-if)#tunnel mode gre multipoint
R2-S(config-if)#ip nhrp network-id 213
R2-S(config-if)#ip nhrp nhs 192.168.1.1
R2-S(config-if)#ip nhrp map 192.168.1.1 10.10.11.1
R2-S(config-if)#ip nhrp shortcut
```

Configuración de DMVPN: DMVPN + IPsec

- ✓ Luego de que los spokes aprenden la dirección del par remoto, el tunel IPsec dinámico se inicia.
- ✓ La configuración es la misma tanto en Hub como spokes

```
R1-H(config)#crypto isakmp policy 10
R1-H(config-isakmp)#encryption aes 256
R1-H(config-isakmp)#authentication pre-share
R1-H(config-isakmp)#group 5

R1-H(config)#crypto isakmp key CCIE address 0.0.0.0

R1-H(config)#crypto ipsec transform-set CCIE esp-aes
R1-H(cfg-crypto-trans)#mode transport

R1-H(config)#crypto ipsec profile DMVPN
R1-H(ipsec-profile)#set transform-set CCIE
```

Configuración de DMVPN: IPv6 in IPv4 Tunnels

```
R20(config)#int tunn0
R20(config-if)#ip add 192.168.1.20 255.255.255.0
R20(config-if)#tunnel source e0/0
R20(config-if)#tunn mode gre multipoint
R20(config-if)#ip nhrp network-id 123
R20(config-if)#ipv6 address 2015:CC1E::20/64
R20(config-if)#ipv6 nhrp network-id 123
```

```
R23(config)#int tunn0
R23(config-if)#ip add 192.168.1.23 255.255.255.0
R23(config-if)#tunnel source e0/0
R23(config-if)#tunnel mode gre multipoint
R23(config-if)#ip nhrp network-id 321
R23(config-if)#ip nhrp nhs 192.168.1.20
R23(config-if)#ip nhrp map 192.168.1.20 10.1.1.20
R21(config-if)#ipv6 address 2015:CC1E::21/64
R21(config-if)#ipv6 nhrp network-id 123
R21(config-if)#ipv6 nhrp nhs 2015:CC1E::20
R21(config-if)#ipv6 nhrp map 2015:CC1E::20/64 10.1.1.20
```

Consideraciones importantes para el enrutamiento con EIGRP y OSPF

Cisco Confidential

Configuración de DMVPN: Usando EIGRP y OSPF

- ✓ **Fase 1:**
  - ❑ **Hub**

```
R1-H(config-if)#ip nhrp map multicast dynamic
R1-H(config-if)#ip ospf net point-to-multipoint
```

  - ❑ **Spoke**

```
R2-S(config-if)#ip nhrp map multicast 10.10.11.1
R2-S(config-if)#ip ospf net point-to-multipoint
```

Configuración de DMVPN: Usando EIGRP y OSPF

- ✓ **Fase 2:**
  - ❑ **Hub** EIGRP

```
R1-H(config-if)#ip nhrp map multicast dynamic
R1-H(config-if)#no ip split-horizon eigrp [#AS]
R1-H(config-if)#no ip next hop-self eigrp [#AS]
```

  - ❑ **Hub** OSPF

```
R1-H(config-if)#ip nhrp map multicast dynamic
R1-H(config-if)#ip ospf network broadcast
R1-H(config-if)#ip ospf priority 255
```

Configuración de DMVPN: Usando EIGRP y OSPF

- ✓ **Fase 2:**
  - ❑ **Spoke**

```
R2-S(config-if)#ip nhrp map multicast 10.10.11.1
R2-S(config-if)#ip ospf network broadcast
R2-S(config-if)#ip ospf priority 0
```

Demo en Vivo: DMVPN /w IPsec en IPv4

Cisco Confidential

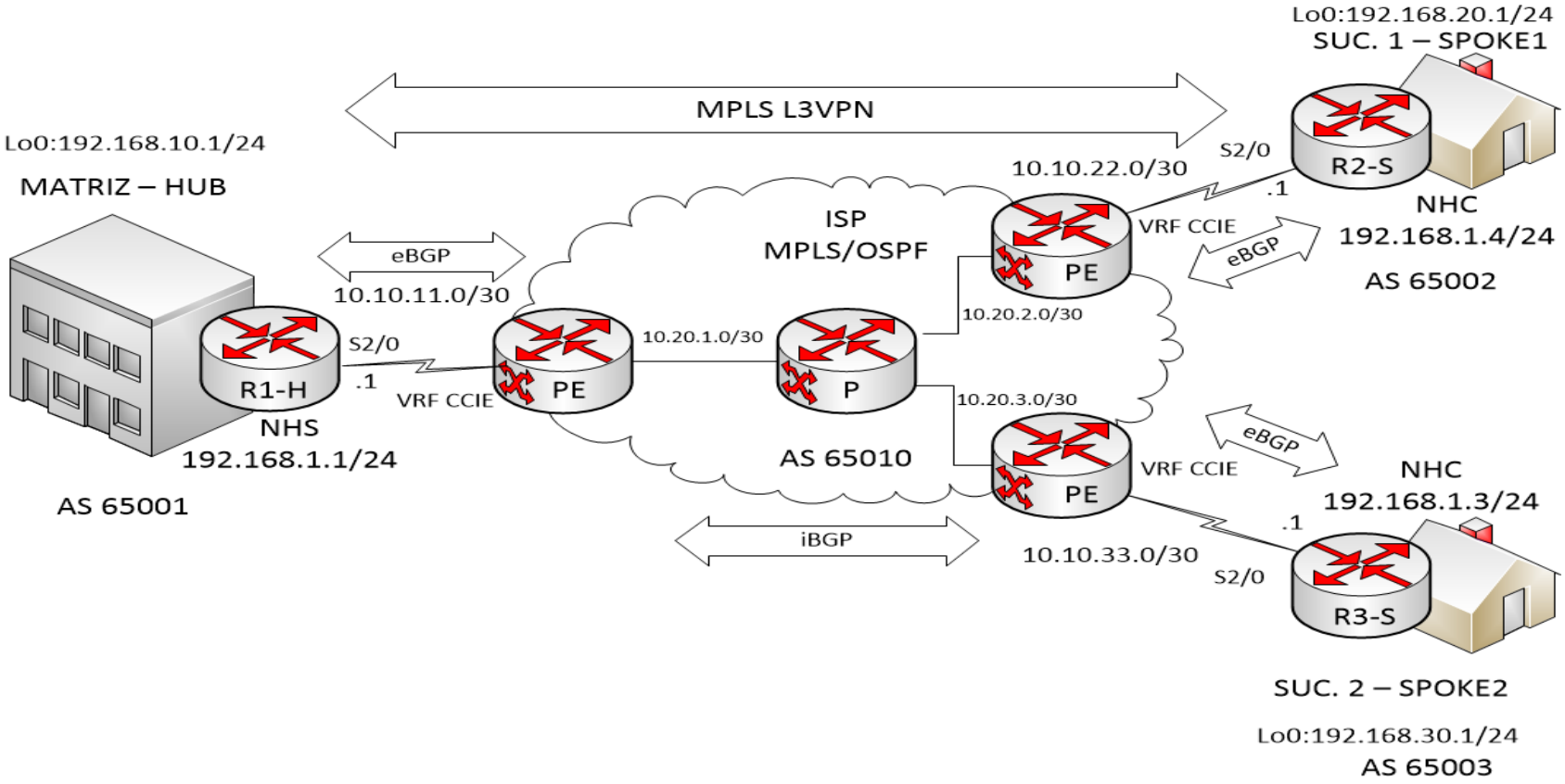
Configuración de DMVPN: Consideraciones de Escalabilidad

- ✓ Usar este tipo de tecnología tiene un impacto en el procesamiento de los equipos, aumento de cabeceras, posibilidad de fragmentación, entre otros, por lo que se recomienda realizar un análisis previo a una implementación (Por ejemplo seguir el Ciclo de vida PPDIOO) y tomar en cuenta las consideraciones de escalabilidad dadas por Cisco para esta tecnología

Guía de diseño para DMVPN

https://supportforums.cisco.com/sites/default/files/legacy/3/9/5/26593-DMVPNbk.pdf

Configuración de DMVPN: Demo en Vivo



Pregunta 3

Una vez atendido el demo en vivo ¿le parece complicada la configuración de DMVPN Fase2 con IPsec?

A. Si
B. No
C. Muy Poco

Q&A

Cisco Confidential

Pregunta 4

¿Implementaría esta solución en la empresa donde labora o recomendaría su implementación a nivel empresarial?

A. Si
B. No
C. Prefiero no contestar

Antes de terminar: Quito, Ecuador

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Antes de terminar: Quito, Ecuador

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Muchas Gracias

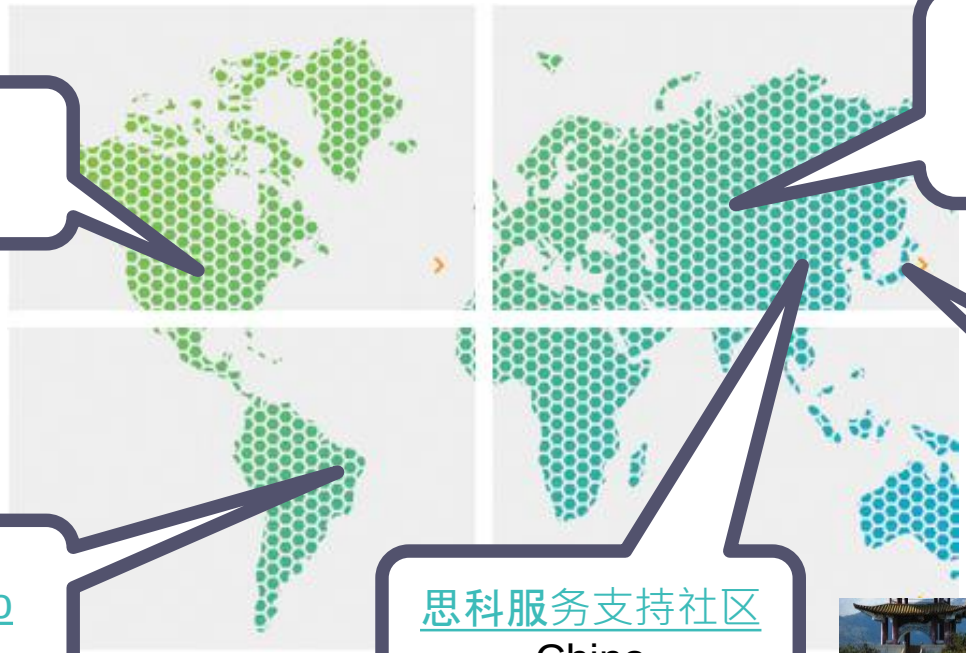
Haga sus preguntas ahora

Utilice el panel de Q&R para realizar sus preguntas

©2016 Cisco and/or its affiliates. All rights reserved.

La Comunidad de Soporte tiene Otros idiomas

Si habla Portugués, Japonés, Ruso, Chino o Inglés lo invitamos a que participe en otro idioma.



Cisco Support Community
Inglés

Сообщество Технической Поддержки Cisco
Ruso

Comunidade de Suporte de Cisco
Portugués

思科服务支持社区
Chino

ツスコサポートコミュニティ
Japonés

Lo invitamos a nuestros próximos eventos en Redes sociales

Cisco TS- Latam

Cisco Mexico

Cisco España

@CiscoTSLatam

@CiscoMexico

@cisco_spain

Cisco Latinoamérica

Cisco Cono Sur

Comunidad Cisco Cansac

CiscoSupportCommunity

@ciscocansacsm

@ciscoconosur

@cisco_support

©2016 Cisco and/or its affiliates. All rights reserved.

Lo invitamos a nuestros próximos eventos en Redes sociales

CiscoLatam

ciscosupportchannel

Cisco Technical Support

CSC-Cisco-Support-Community

©2016 Cisco and/or its affiliates. All rights reserved.

¡Únete a la Comunidad de Soporte de Cisco!

Aquí puedes resolver dudas técnicas, encontrar información en documentos, blogs y videos con contenidos técnicos totalmente en español, además de poder colaborar e interactuar en tiempo real con los expertos en tecnología.

Documentos

Discusiones

Blogs

Móvil

Video

Pregunte al Experto

©2016 Cisco and/or its affiliates. All rights reserved.

¡Nos interesa su opinión!

Para completar la evaluación espere un momento y aparecerá automáticamente al cerrar el browser de la sesión

©2016 Cisco and/or its affiliates. All rights reserved.

¡Gracias por su tiempo!

Por favor tome un momento para contestar la evaluación

CISCO